



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/865,884

05/25/2001

Mark Depp

BOS-31032(1)

8022

22202

7590

07/01/2004

WHYTE HIRSCHBOECK DUDEK S C  
555 EAST WELLS STREET  
SUITE 1900  
MILWAUKEE, WI 53202

EXAMINER

SIANGCHIN, KEVIN

ART UNIT

PAPER NUMBER

2623

DATE MAILED: 07/01/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

# Office Action Summary

Application No.

09/865,884

Applicant(s)

DEPP ET AL.

Examiner

Kevin Siangchin

Art Unit

2623

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☐ Responsive to communication(s) filed on \_\_\_\_.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-60 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_ is/are allowed.
- 6) ☐ Claim(s) \_\_\_\_ is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 29 May 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date 5/\_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_

## Detailed Action

### *Claims*

#### Objections

1. Claims 16, 18, 21, and 27 are objected to because of the following informalities. The claims refer to the "biometric *system* of claim 13". Claim 13, on the hand, claims a biometric *network*. Similar changes in the claims that depend on claims 16, 18, 21, and 27 should also be made. Claims that are dependant on claim 13 will be assumed, henceforth, to claim biometric systems. Appropriate correction is required.
2. Claim 28 is objected to because of the following informalities. In claim 28, the Applicant mentions "a transaction history data store" twice, where clearly one mention was intended. Appropriate correction is required.

#### Rejections Under 35 U.S.C. § 112(1)

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 27-28 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.
5. According to claims 27-28, the software programmed into the biometric device includes a report generation module, which, in turn, implies that report generation occurs at the biometric device. However, it is clear from Figs. 1-2 of the Applicant's disclosure that report generation occurs at the central data center and not at the location of the biometric device(s). The Applicant's specification, therefore, does not enable this feature of the Applicant's claimed invention.

Rejections Under 35 U.S.C. § 102(e)

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1-2, 4-5, 13, 16-19, 29-32, 42-47, 49-52, and 54-58 are rejected under 35 U.S.C. 102 <sup>(b)</sup>~~(a)~~ as being anticipated by DiMaria et al. (U.S. Patent 5,959,541).

8. *The following is in regard to Claim 1.* DiMaria et al. discloses a biometric time and attendance system that includes:

(1.a.) At least one biometric device (e.g. EPIDERMAL TOPOGRAPHICAL SCANNER 12, depicted in DiMaria et al. Fig. 2, present in each terminal 10 or the biometric system) capable of identifying a user and generating data related to the user. See DiMaria et al. Figs. 1-2. For the remainder of this document, EPIDERMAL TOPOGRAPHICAL SCANNER will be referred to, interchangeably, as ETS.

(1.b.) A central data center (e.g. HOST 20, depicted in DiMaria et al. Fig. 1) in communication with the at least one biometric device (e.g. ETS 12 of the terminals 10, depicted in DiMaria et al. Fig. 1) for receiving the generated data. See DiMaria et al. Figs. 1-2 and column 4, lines 1-39.

(1.c.) The generated data relates to time and attendance information with respect to the user. See, for example, DiMaria et al. column 4, lines 1-39. Note that this data may be resident on the terminal, as well as the host. See DiMaria et al. column 5, lines 15-16.

It has thus been shown that the biometric time and attendance system of DiMaria et al. conforms to biometric system proposed in claim 1. In this way, the teachings of DiMaria et al. anticipate the biometric system put forth in claim 1.

9. *The following is in regard to Claim 2.* As shown above, DiMaria et al. disclose a biometric system that is in accordance with claim 1. Furthermore, the time and attendance information of DiMaria et al.'s system includes user name (e.g. the identity of the individual – DiMaria et al. column 4, line 15), a location (DiMaria et al. column 4, line 27), an entrance time (DiMaria et al. Fig. 3B, step 9A), and an exit time (DiMaria et al. Fig. 3B, step 9A). Clearly, a time-stamp must also be included in order to quantify the entrance and exit times. The biometric time and attendance system of DiMaria et al. thus conforms to that which is put forth in claim 2.

10. *The following is in regard to Claim 4.* As shown above, DiMaria et al. disclose a biometric system that is in accordance with claim 4. Furthermore, in DiMaria et al.'s biometric system, the biometric device compares stored biometric data (DiMaria et al. column 3, lines 18-19) to live biometric data (DiMaria et al. Fig. 3A, step S7). Clearly, it would be reasonable to assume that (hopefully) living individuals are intended to access the time and attendance system of DiMaria et al. Assuming this is the case, the biometric data of the user would constitute live biometric data. The biometric time and attendance system of DiMaria et al. thus conforms to that which is put forth in claim 4.

11. *The following is in regard to Claim 5.* As shown above, DiMaria et al. disclose a biometric system that is in accordance to that which is put forth in claim 4. According to DiMaria et al. (DiMaria et al. column 3, lines 19-21), the aforementioned ETS may be a fingerprint scanner, thus implying that the stored and live biometric data is that of a fingerprint. In this way, The biometric time and attendance system of DiMaria et al. conforms to that which is put forth in claim 4.

12. *The following is in regard to Claim 13.* DiMaria et al. discloses a biometric time and attendance system that includes:

- (13.a.) At least one biometric unit that compares live biometric data with stored biometric data to generate time and attendance data. See the discussion above relating to (1.a), (1.c), and claim 4.
- (13.b.) A central data center in communication with the biometric device. See the discussion above relating to (1.b).

- (13.c.) Software programmed into the biometric device and operational with the central data center to facilitate communication between the biometric device and the central data center. This is feature implicit to the discussion in DiMaria et al. column 3, lines 36-47.

Lastly, note that DiMaria et al.'s system is in a network configuration (note DiMaria et al. Fig. 1) consisting of multiple terminals connected a central host. Consequently, the time and attendance system of DiMaria et al. can be regarded as a biometric network for use in time and attendance applications. Taking into account the discussion above, it has been shown that the biometric time and attendance system of DiMaria et al. conforms to biometric network proposed in claim 13. In this way, the teachings of DiMaria et al. anticipate the biometric network put forth in claim 13.

13. *The following is in regard to Claim 16.* As shown above, DiMaria et al. disclose a biometric time and attendance system that conforms to the biometric network of claim 13. DiMaria et al.'s system is further programmed to capture transactional data, such as entry and/or exit times and locations, from the biometric network. See, for example, DiMaria et al. column 4, lines 12-39 and column 5, lines 15-16. The components of DiMaria et al.'s system that are involved in capturing these data would constitute an "acquisition module". In this way, the biometric time and attendance system of DiMaria et al. conforms to biometric network proposed in claim 16.

14. *The following is in regard to Claim 17.* As shown above, DiMaria et al. disclose a biometric time and attendance system that conforms to the biometric network of claim 16. DiMaria et al.'s system is further programmed (e.g. in Fig. 3B, step S9A and/or step S7B) to send information related to the transactional data into a database in the central data center. Since this database contains transactional history data, it can be considered a "transactional history data store". In this way, the biometric time and attendance system of DiMaria et al. conforms to biometric network proposed in claim 16.

15. *The following is in regard to claim 18.* As shown above, DiMaria et al. disclose a biometric time and attendance system that conforms to the biometric network of claim 13. DiMaria et al.'s system is further programmed to enter and edit employee information (e.g. via keypad 16 of DiMaria et al. Fig. 6) from the biometric network. See, for example, DiMaria et al. Fig. 3B, step S13, Fig. 7A, step S5, and column, lines 13-15 and lines 55-67. The components of DiMaria et al.'s system that are involved in this

process would constitute an “employee data maintenance module”. In this way, the biometric time and attendance system of DiMaria et al. conforms to biometric network proposed in claim 18.

16. *The following is in regard to Claim 19.* As shown above, DiMaria et al. disclose a biometric time and attendance system that conforms to the biometric network of claim 18. DiMaria et al.’s system is further programmed (e.g. as indicated by step S15 in DiMaria et al. Fig. 3B) to send employee information into a database (e.g. database 60 – DiMaria et al. Fig. 1) in the central data center (e.g. HOST 20 – DiMaria et al. Fig. 1). Since this database stores employee information, it can be considered an “employee information data store.” In this way, the biometric time and attendance system of DiMaria et al. conforms to biometric network proposed in claim 19.

17. *The following is in regard to Claim 29.* DiMaria et al. discloses a biometric time and attendance system that includes:

(29.a.) At least one biometric device for comparing live biometric data to stored biometric data and generating time and attendance data based on the comparison. See the discussion above relating to (13.a).

(29.b.) A central data center in communication with the biometric device for receiving the time and attendance data from the biometric device. See the discussion above relating to (13.b)-(13.c)

Taking into account the discussion above (primarily with regard to claim 13), it has been shown that the biometric time and attendance system of DiMaria et al. conforms to biometric network proposed in claim 29. In this way, the teachings of DiMaria et al. anticipate the biometric system put forth in claim 29.

18. *The following is in regard to Claim 30.* As shown above, DiMaria et al. disclose a biometric time and attendance system that conforms to the biometric system of claim 29. The time and attendance data of DiMaria et al.’s system consists of an entry-time and an exit-time. See DiMaria et al. column 4, lines 12-19. Note that a check-in time is essentially the same as an entry-time. Further note that, since the system of DiMaria et al. logs user access and user egress (e.g. step S10A in DiMaria et al. Fig. 3B), a user’s presence at a given location is essentially logged. Therefore, the logged entry and exit times represent attendance

data. In this way, the biometric time and attendance system of DiMaria et al. conforms to biometric system proposed in claim 30.

19. *The following is in regard to Claims 31-32.* The subject matter of claims 31 and 32 deviates from that of claims 29 and 30, respectively, only in that the source of biometric data is specifically a user's fingerprint. Therefore, arguments presented above with regard to claims 29-30 are applicable here. Given those arguments and the fact that a fingerprint is the biometric source of choice in DiMaria et al.'s system (DiMaria et al. column 3, lines 57-58), the biometric time and attendance system of DiMaria et al. conforms to biometric system proposed in claim 31-32.

20. *The following is in regard to Claim 49.* DiMaria et al. discloses a method for tracking time and attendance using biometric input from users. DiMaria et al.'s method includes:

- (49.a.) Providing at least one biometric device (e.g. ETS 12 of TERMINAL 10 shown in DiMaria et al. Fig. 2). See, for example, DiMaria et al. Figs. 1-2.
- (49.b.) The biometric device compares live biometric data with stored biometric data to generate (e.g. step S7 of DiMaria et al. Fig. 3A) time and attendance data. See, for example, DiMaria et al. column 4, lines 1-39. Note that this data may be resident on the terminal, as well as the host. See DiMaria et al. column 5, lines 15-16.
- (49.c.) Communicating the time and attendance data to a central data center (e.g. HOST 20 depicted in DiMaria et al. Fig. 1) in communication with the at least one biometric device. See DiMaria et al. Figs. 1-2 and column 4, lines 1-39.

Lastly, note that, in the time and attendance method of DiMaria et al., time and attendance reports are generated (e.g. step 9A or 10B of DiMaria et al. Fig. 3A). Consequently, the time and attendance method of DiMaria et al. can be regarded as a method of biometric time and attendance reporting. It has thus been shown that the biometric time and attendance method of DiMaria et al. conforms to the method of biometric time and attendance reporting of claim 49. In this way, the teachings of DiMaria et al. anticipate the method put forth in claim 49.

21. *The following is in regard to Claim 50.* As shown above, DiMaria et al. disclose a biometric time and attendance method that conforms to the method of biometric time and attendance reporting proposed in



claim 49. DiMaria et al.'s method further includes generating a report using the time and attendance data. See, for example, step 9A or 10B of DiMaria et al. Fig. 3A and the discussion above with regard to the attendance data of claim 30. Therefore, the biometric time and attendance method of DiMaria et al. conforms to the method of biometric time and attendance reporting proposed in claim 50.

22. *The following is in regard to Claim 51.* As shown above, DiMaria et al. disclose a biometric time and attendance method that conforms to the method of biometric time and attendance reporting proposed in claim 49. As noted earlier, the fingerprint is the biometric source of choice in DiMaria et al.'s system (DiMaria et al. column 3, lines 57-58). Therefore, in the method of DiMaria et al., the live and stored biometric data are fingerprint data. This is in accordance with claim 51.

23. *The following is in regard to Claim 52.* DiMaria et al. discloses a method for tracking time and attendance using biometric input from users. DiMaria et al.'s method includes:

- (52.a.) Providing at least one biometric device. See, for example, DiMaria et al. Figs. 1-2.
- (52.b.) Biometrically identifying a user (e.g. step S7-S8 in DiMaria et al. Figs 3A-3B) and generating data related to the user (e.g. step 9A in DiMaria et al. Fig 3B).
- (52.c.) Communicating the data to a central data center (e.g. HOST 20 depicted in DiMaria et al. Fig. 1) in communication with the at least one biometric device (e.g. step S6 of DiMaria et al. Fig. 3A). See DiMaria et al. Figs. 1-2 and column 4, lines 1-39.

Lastly, note that, in the time and attendance method of DiMaria et al., time and attendance reports are generated (e.g. step 9A or 10B of DiMaria et al. Fig. 3A). Consequently, the time and attendance method of DiMaria et al. can be regarded as a method of biometric time and attendance reporting. It has thus been shown that the biometric time and attendance method of DiMaria et al. conforms to the method of biometric time and attendance reporting of claim 52. In this way, the teachings of DiMaria et al. anticipate the method put forth in claim 52.

24. *The following is in regard to Claim 54.* As shown above, DiMaria et al. disclose a biometric time and attendance method that conforms to the method of biometric time and attendance reporting proposed in claim 52. As noted earlier, the fingerprint is the biometric source of choice in DiMaria et al.'s system (DiMaria et al. column 3, lines 57-58). Therefore, in the method of DiMaria et al., the biometrically

identifying step (step (52.b) above) may include taking fingerprint data from the user. This is in accordance with the method of claim 54.

25. *The following is in regard to Claim 55.* DiMaria et al. discloses a method for tracking time and attendance (i.e. “a method of monitoring time and attendance activities”) using biometric input from users. DiMaria et al.’s method includes:

- (55.a.) Providing at least one biometric device. See, for example, DiMaria et al. Figs. 1-2. According to DiMaria et al. (DiMaria et al. column 3, lines 22-23), “each terminal 10 [DiMaria et al. Fig. 1] is placed at a location where access control is desired”.
- (55.b.) Biometrically identifying a user (e.g. step S7-S8 in DiMaria et al. Figs 3A-3B) and generating data related to the user (e.g. step 9A in DiMaria et al. Fig 3B).
- (55.c.) Communicating the data to a central data center (e.g. HOST 20 depicted in DiMaria et al. Fig. 1) in communication with the at least one biometric device (e.g. step S6 of DiMaria et al. Fig. 3A). See DiMaria et al. Figs. 1-2 and column 4, lines 1-39.
- (55.d.) Receiving data from the biometric devices. Clearly, the host receives the transmitted biometric and personal identification data from the terminal(s) (e.g. step S10 of DiMaria et al. Fig. 7A).
- (55.e.) Processing the data. Clearly, transmitted data are processed.

The data (e.g. time of entry/exit) represents information related to the attendance of the user at the particular location. See the discussion above with regard to the attendance data of claim 30. It has thus been shown that the biometric time and attendance method of DiMaria et al. conforms to the method of biometric time and attendance monitoring of claim 55. In this way, the teachings of DiMaria et al. anticipate the method put forth in claim 55.

26. *The following is in regard to Claim 56.* As shown above, DiMaria et al. disclose a biometric time and attendance method that conforms to the method of claim 55. In the method, the information is generated relating to when the identifying of the user occurs (e.g. user access/egress times) at the particular location. Note, for example, steps S10-S10A of DiMaria et al. Fig. 3B. In this way, the biometric time and attendance method of DiMaria et al. conforms to that which is put forth in claim 56.

27. *The following is in regard to Claim 57.* As shown above, DiMaria et al. disclose a biometric time and attendance method that conforms to the method of claim 55. DiMaria et al.'s method generates a report using the data relating to the user (e.g. steps 9B or 10A of DiMaria et al. Fig. 3B). Therefore, the biometric time and attendance method of DiMaria et al. conforms to that which is put forth in claim 57.

28. *The following is in regard to Claim 58.* As shown above, DiMaria et al. disclose a biometric time and attendance method that conforms to the method of claim 55. In the method of DiMaria et al., comparison is made between stored biometric data to live biometric data. See the discussion above with regard to claim 4. Taking this into account, it is evident that the biometric time and attendance method of DiMaria et al. conforms to that which is put forth in claim 58.

29. *The following is in regard to Claim 42.* DiMaria et al. discloses a biometric time and attendance system. This system generates a report(s) that includes:

(42.a.) Timing data (e.g. access/egress times – note steps S12-S12B or steps 13-13A of DiMaria et al. Fig. 7B) derived from a comparison (e.g. steps S10-S10A of DiMaria et al. Fig. 7A) of live biometric data to stored biometric data.

(42.b.) Identification data (e.g. identification information and/or personal identification code – note step S10 of DiMaria et al. Fig. 7A) derived from the comparison of live biometric data to stored biometric data.

See DiMaria et al. column 4, lines 14-15 and lines 26-28. It has thus been shown that report generated by the biometric time and attendance system of DiMaria et al. conforms to the report of claim 42. In this way, the teachings of DiMaria et al. anticipate the time and attendance report put forth in claim 42.

30. *The following is in regard to Claim 43.* The subject matter of claim 43 deviates from that of claim 42 only in that the source of biometric data is specifically a user's fingerprint. Therefore, arguments presented above with regard to claim 42 are applicable here. Given those arguments and the fact that a fingerprint is the biometric source of choice in DiMaria et al.'s system (DiMaria et al. column 3, lines 57-58), the biometric time and attendance system of DiMaria et al. conforms to biometric system proposed in claim 43.

31. *The following is in regard to Claim 44.* DiMaria et al. discloses a biometric time and attendance system. This system generates a report(s), for use with a biometric device(s), that includes:

(44.a.) Timing data. See the discussion above relative to (42.a).

(44.b.) Identification data. See the discussion above relative to (42.b). Note that this data and the timing data are related in that both are attributed to a single user.

Both of these data are generated by the biometric device(s). As indicated previously, timing data may be generated by the terminals of DiMaria et al.'s system (DiMaria et al. column 5, lines 15-16). Identification data, such as a personal identification code (see step S5 in DiMaria et al. Fig. 7A), is generated via the keypad supplied at each terminal. The report, which includes both of these data, is generated as a result of biometric verification (e.g. step 12B of DiMaria et al. Fig. 7B). In this way, the report(s) generated by the biometric time and attendance system of DiMaria et al. conforms to the report of claim 44. The teachings of DiMaria et al. anticipate the time and attendance report put forth in claim 44.

32. *The following is in regard to Claim 45.* The subject matter of claim 45 deviates from that of claim 44 only in that the source of biometric data is specifically a user's fingerprint. Therefore, arguments presented above with regard to claim 44 are applicable here. Given those arguments and the fact that a fingerprint is the biometric source of choice in DiMaria et al.'s system (DiMaria et al. column 3, lines 57-58), the biometric time and attendance system of DiMaria et al. conforms to biometric system proposed in claim 45.

33. *The following is in regard to Claim 46.* DiMaria et al. discloses a biometric time and attendance system. This system generates a report(s), for use with a biometric device(s), that includes:

(46.a.) Entrance/Exit times (or check-in/check-out times). Note, for example, steps S9-9B of DiMaria et al. Fig. 3B.

(46.b.) Personal/User identification (DiMaria et al. column 4, lines 14-15 and lines 26-28). As indicated by DiMaria et al. (DiMaria et al. Fig. 7A, step S5), this may include a personal identification code (which could represent a payroll in payroll applications – e.g. DiMaria et al. column 4, lines 36-39). Clearly, such data could also include a user's name.

These data are generated in a report upon user verification (e.g. steps S12-S12B in DiMaria et al. Fig. 7B).

In this manner, In this way, the report(s) generated by the biometric time and attendance system of DiMaria et al. conforms to the report of claim 46. The teachings of DiMaria et al. anticipate the time and attendance report put forth in claim 46.

34. *The following is in regard to Claim 47.* As shown above, DiMaria et al. disclose a time and attendance report that conforms to that which is put forth in claim 46. As noted above, biometric verification, in the system of DiMaria et al., is preferably in the form of user fingerprint verification. Given this, it should be clear that the report(s) generated by the biometric time and attendance system of DiMaria et al. conforms to the report proposed in claim 47.

Rejections Under 35 U.S.C. § 103(a)

35. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

36. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over DiMaria et al., in view of Nocker (U.S. Patent 6,236,486).

37. *The following is in regard to Claim 3.* As shown above, DiMaria et al. disclose a biometric time and attendance system that conforms to the biometric system of claim 1. While DiMaria et al.'s system is in a network configuration (note DiMaria et al. Fig. 1) consisting of multiple terminals connected a central host, and despite the fact that serial, wireless, modems and Internet are well-known networking technologies, DiMaria et al. does not expressly show or suggest that the central data center is in communication with the biometric device via one of a serial connection, a wireless connection, a modem, an Ethernet connection and an Internet connection.

38. According to Nocker (Nocker column 1, lines 6-12), "[i]n the automated identification and data capture industry, it is known to operate a wireless local area network (LAN) that includes a plurality of

handheld data-collection terminals [e.g. the aforementioned biometric device(s)] that communicate over a radio frequency (RF) channel with a central host computer [e.g. the aforementioned central data center] ... Such wireless LAN systems are particularly well suited to data capture applications [such as]... time and attendance monitoring”.

39. These teachings of Nocker are applicable to those of DiMaria et al. because they are analogous art. In particular, the teachings of Nocker (especially Nocker’s Background), like those of DiMaria et al., are directed toward a network topology consisting of a plurality of data-collection terminals logically connected to a central host computer or data center. Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the applicant’s claimed invention, to logically connect the various biometric terminals (e.g. terminals 10 of DiMaria et al. Fig. 1) of DiMaria et al.’s time and attendance system to the central data center (e.g. host 20 of DiMaria et al. Fig. 1) via wireless LAN technology, as suggested by Nocker. The motivation to use wireless LAN technology would have been to eliminate cumbersome wiring and, as a result, allow the biometric terminals to have non-stationary positions. Networking the host and terminals of DiMaria et al.’s time and attendance system using wireless LAN technology would yield a time and attendance system that satisfies the limitations of claim 3.

40. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over DiMaria et al., in view of Schmitt et al. (U.S. Patent 6,088,585).

41. *The following is in regard to Claim 7.* As shown above, DiMaria et al. disclose a biometric time and attendance system that conforms to the biometric system of claim 1. DiMaria et al., however, do not show or suggest that the biometric device be part of a telephone.

42. Schmitt et al. disclose a portable telecommunication device that includes a fingerprint sensor. This device takes the form of a cellular telephone (e.g. cellular telephone 190 of Schmitt et al. Fig. 14).

43. The teachings of Schmitt et al. and DiMaria et al. are combinable because they are analogous art. More precisely, the teachings of Schmitt et al. and DiMaria et al. are both directed toward devices and/or systems that verify a user(s) identity via biometric input. Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the applicant’s claimed invention, to structure the biometric device(s)

of DiMaria et al.'s time and attendance system so that the device(s) is part of a cellular telephone, such as that of Schmitt et al. The motivation to do so would have been to provide time and attendance tracking, as well as secure access to a given location, using pre-existing cellular technology. Therefore, the time and attendance system, obtained by combining the teachings of the Schmitt et al. and DiMaria et al. in the manner discussed above, conforms to system of claim 7.

44. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over DiMaria et al., in view of Maes et al. (U.S. Patent 6,016,476).

45. *The following is in regard to Claim 8.* As shown above, DiMaria et al. disclose a biometric time and attendance system that conforms to the biometric system of claim 1. DiMaria et al., however, do not show or suggest that the biometric device be part of a personal digital assistant (PDA).

46. Maes et al. disclose a PDA device that utilizes biometric security to provide user verification (see Maes et al. column 2, lines 31-33).

47. The teachings of Maes et al. and DiMaria et al. are combinable because they are analogous art. More precisely, the teachings of Maes et al. and DiMaria et al. are both directed toward devices and/or systems that verify a user(s) identity via biometric input. Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the applicant's claimed invention, to structure the biometric device(s) of DiMaria et al.'s time and attendance system so that the device is part of a PDA, as suggested by Maes et al. The motivation to do so would have been to provide users with the extensive functionality offered by a PDA, while still accommodating time and attendance tracking, as well as secure access to a given location. Therefore, the time and attendance system, obtained by combining the teachings of the Maes et al. and DiMaria et al. in the manner discussed above, conforms to system of claim 8.

48. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over DiMaria et al., in view of Srey et al. (U.S. Patent 6,141,436).

49. *The following is in regard to Claim 9.* As shown above, DiMaria et al. disclose a biometric time and attendance system that conforms to the biometric system of claim 1. DiMaria et al., however, do not show or suggest that the biometric device include a biometric authentication device with a button for fingerprint data storage.

50. Srey et al. disclose a biometric device (e.g. portable communication device 100 depicted in Srey et al. Fig. 2 or portable communication device 700 of Fig. 2 ) including a biometric authentication device (e.g. fingerprint identification system 709 shown in Srey et al. Fig. 7) with a button (e.g. the switch 201 and scanner 115 arrangement depicted in Srey et al. Fig. 2 and discussed in column 4, lines 6-10, 20-22) for fingerprint data storage (e.g. on first memory device 705 – see Srey et al. Fig. 7 and column 4, lines 67 to column 5, lines 1-6).

51. The teachings of Srey et al. and DiMaria et al. are combinable because they are analogous art. More precisely, the teachings of Srey et al. and DiMaria et al. are both directed toward devices and/or systems that verify a user(s) identity via biometric input. Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the applicant's claimed invention, to structure the biometric device(s) of DiMaria et al.'s time and attendance system so that the device(s) include a biometric authentication device with a button for fingerprint data storage, as illustrated by Srey et al. (Srey et al. Fig. 2). Since the fingerprint sensor is activated only upon depressing the switch, such a configuration would advantageously conserve power. By structuring the biometric device(s) of DiMaria et al.'s time and attendance system as just described, one would obtain a biometric time and attendance system that conforms to that which is put forth in claim 9.

52. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over DiMaria et al., in view of Setlak et al. (U.S. Patent 5,828,773).

53. *The following is in regard to Claim 11.* As shown above, DiMaria et al. disclose a biometric time and attendance system that conforms to the biometric system of claim 1. DiMaria et al., however, do not show or suggest that the biometric device be a laptop computer.

54. Setlak et al. disclose a biometric device that is laptop. See Setlak et al. Fig. 25.



55. The teachings of Setlak et al. and DiMaria et al. are combinable because they are analogous art. More precisely, the teachings of Setlak et al. and DiMaria et al. are both directed toward devices and/or systems that verify a user(s) identity via biometric input. Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the applicant's claimed invention, to structure the biometric device(s) of DiMaria et al.'s time and attendance system so that the device is a laptop, as suggested by Setlak et al. The motivation to do so would have been to provide users with the extensive functionality offered by a laptop, while still accommodating time and attendance tracking, as well as secure access to a given location. Therefore, the time and attendance system, obtained by combining the teachings of the Setlak et al. and DiMaria et al. in the manner discussed above, conforms to system of claim 8.

56. Claims 12, 14-15, and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over DiMaria et al., in view of Biometric Identification's Veriprint™ 2100 (described in "Biometric Identification Veriprint™ 2100, Installation and Operation Manual", 1999). Note that, henceforth in this document, the latter reference will be referred to as the Veriprint Operation Manual.

57. *The following is in regard to Claim 12.* As shown above, DiMaria et al. disclose a biometric time and attendance system that conforms to the biometric system of claim 1. DiMaria et al., however, do not show or suggest that the biometric device be part of a time clock.

58. The Veriprint 2100 is a biometric user verification system with time and attendance system functionalities. According to the Veriprint Operation Manual (page 6), the Veriprint 2100 can be used as a simple punch clock. In this manner, the biometric device (e.g. the Veriprint 2100 terminal shown on page 2, Fig. 1 of the Veriprint Operation Manual) is part of a time clock, namely a punch clock.

59. The Veriprint Operation Manual and DiMaria et al. are combinable because they are analogous art. Specifically, DiMaria et al. and the Veriprint Operation Manual propose security and/or user-logging systems, using biometric verification, that find particular usage in time and attendance applications (see the Veriprint Operation Manual, page 108). Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the applicant's claimed invention, to structure the biometric device of DiMaria et al.'s time and attendance system in a manner similar to the Veriprint 2100, so that the biometric device is at

least part of a punch clock. The motivation for doing so would have been to provide the user with visual feedback as to what time he/she is logging in or otherwise accessing the time and attendance system. Configuring the biometric device of DiMaria et al.'s time and attendance system in this manner would produce a biometric time and attendance system in accordance with claim 12.

60. *The following is in regard to Claim 14.* As shown above, DiMaria et al. disclose a biometric time and attendance system that conforms to the biometric network of claim 13. DiMaria et al., however, does not show or suggest that the software include a configuration module for describing the configuration of the biometric network.

61. The Veriprint™ 2100 allows administration and configuration of the biometric network from and individual Veriprint™ 2100 unit. See, for example, the discussion found on page 44 of the Veriprint Operation Manual. The various components of the Veriprint™ 2100 that facilitate this configuration and administration capability could collectively be regarded as a configuration module.

62. The Veriprint Operation Manual and DiMaria et al. are combinable because they are analogous art. Specifically, DiMaria et al. and the Veriprint Operation Manual propose security and/or user-logging systems, using biometric verification, that find particular usage in time and attendance applications (see the Veriprint Operation Manual, page 108). Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the applicant's claimed invention, to incorporate a configuration and administration functionality into the time and attendance system of DiMaria et al. The motivation to do so would have been to allow certain users the ability to, among other things, change the security level (the Veriprint Operation Manual page 63) or set network properties (e.g. baud rate – the Veriprint Operation Manual page 74). Incorporating a configuration and administration functionality, similar to that of the Veriprint™ 2100, into the time and attendance system of DiMaria et al. would yield a system in accordance with claim 14.

63. *The following is in regard to Claim 15.* As shown above, the teachings of the Veriprint Operation Manual and DiMaria et al., when combined in the manner discussed above, satisfy the limitations of claim 14. Clearly, in order to effect the desired network configuration, information related to the configuration of the biometric network must be stored. To ensure proper operation of the network, each node (e.g. the terminals and host of DiMaria et al.'s system) of the network must "aware", at least in part, of the network

configuration. Therefore, at least a portion of the network configuration information must be stored at each of the network nodes. The storage, in each of these components, may be referred to as a “a biometric network description data store”. Hence, the storage of information related to the configuration of the biometric network in a biometric network description data store, is inherent to any time and attendance network having a network configuration and/or administration capability. Therefore, the time and attendance network, obtained by combining the teachings of the Veriprint Operation Manual and DiMaria et al., in the manner discussed above, conforms to that which is put forth in claim 15.

64. *The following is in regard to Claim 48.* As shown above, DiMaria et al. disclose a time and attendance report that conforms to that which is put forth in claim 46. The generation of this data, in the form of the aforementioned report, is contingent upon a comparison of live biometric data to stored biometric data. Though, it would be exceedingly apparent to one of ordinary skill in the art that the stored biometric data and its comparison to the live biometric data could occur at the biometric device, DiMaria et al. does not show or suggest this. Instead, in DiMaria et al.’s system the stored data and comparison occur at the host (i.e. the central data center).

65. Several systems exist where the stored biometric data and its comparison to live biometric data are resident on a client device capable of capturing biometric data. An example of such a product is the Veriprint™ 2100. See the Veriprint Operation Manual, page 2, *About the Veriprint™ 2100*. In the Veriprint™ 2100, comparison is made between live fingerprint data with fingerprint templates stored on board the Veriprint™ 2100.

66. The Veriprint Operation Manual and DiMaria et al. are combinable because they are analogous art. Specifically, DiMaria et al. and the Veriprint Operation Manual propose security and/or user-logging systems, using biometric verification, that have time and attendance functionality (see the Veriprint Operation Manual, page 108). Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the applicant's claimed invention, to have both the stored biometric data and the comparison of this data with live biometric data occur on the biometric device, as in the Veriprint™ 2100. The advantage of such a configuration would have been to reduce, or even eliminate, any potential lag in data communication that may occur between the client biometric device and the central data center.

Furthermore, this configuration would introduce and advantageous level of data redundancy so that user access or egress may occur despite a potential loss of connection to the data center. The biometric time and attendance system of DiMaria et al., when modified in the manner just described, would be generate time and attendance reports wherein the data is derived from a comparison of live biometric data to stored biometric data *at the biometric device*. Such reports would be in accordance with claim 48.

67. Claims 21-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over DiMaria et al., in view of Biometric Identification's Veriprint™ 2000 (described in "The Veriprint™ 2000 Fingerprint Verification System: User's Guide, Version 2.31", 1998). Note that, henceforth in this document, the latter reference will be referred to as the Veriprint User Guide.

68. *The following is in regard to Claim 21.* As shown above, DiMaria et al. disclose a biometric time and attendance system that conforms to the biometric network of claim 13. However, the time and attendance system of DiMaria et al. does not, as explicitly disclosed, permit the input and editing of company data information.

69. The Veriprint 2000 is a biometric user verification system with time and attendance system functionality. The Veriprint 2000 allows users to enter and edit their departmental information using a *Transfer Dept.* function (Veriprint User Guide, page 6). Also, departments can be added and deleted from a *department list* (Veriprint User Guide, page 98). Clearly, these departments and departmental codes represent "company data information".

70. The Veriprint User Guide and DiMaria et al. are combinable because they are analogous art. Specifically, DiMaria et al. and the Veriprint User Guide propose security and/or user-logging systems, using biometric verification, that are particularly useful in time and attendance applications. Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the applicant's claimed invention, to augment the operation of DiMaria et al.'s time and attendance system to accommodate company data information, such as the departmental information used in the Veriprint 2000, and user entry and editing of that information. The motivation to do so would have been to ascribe additional and potentially important departmental information to users. The components of the system, obtained in this manner, that involve the

entry and editing of company information would constitute a “company data maintenance module program”. This could, for instance, further be used to further identify a user. Extending the functionality of the time and attendance system of DiMaria et al. in the manner just discussed, would yield a biometric time and attendance network that conforms to that which is claimed in claim 21.

71. *The following is in regard to Claim 22.* As shown above, the time and attendance system of DiMaria et al. can be modified according to the teachings of the Veriprint User Guide, to produce a time and attendance network that satisfies the limitations of claim 21. As stated above with respect to claim 21, the Veriprint 2000 allows departments to be added and deleted from a *department list* (Veriprint User Guide, page 98). This department list can be reasonably interpreted as representing a “company information data store”. Although not explicitly shown in the Veriprint User Guide, it would be obvious to one of ordinary skill in the art that the department list or company information data store could be stored on a central data center, particularly given the framework of DiMaria et al.’s time and attendance system. The motivation to do so would have been to simplify the structure of the aforementioned biometric devices, to accommodate a larger set of company information data with presumably larger storage at the central data center, and/or to provide company information data redundancy and persistence. Taking this into account and the teachings of DiMaria et al. and the Veriprint User Guide, the time and attendance system, obtained by combining the teachings of DiMaria et al. and the Veriprint User Guide with the provision that company information data (department lists) be stored on a central data center, would be in accordance with claim 22.

72. *The following is in regard to Claim 23.* As shown above, the time and attendance system of DiMaria et al. can be modified according to the teachings of the Veriprint User Guide, to produce a time and attendance network that satisfies the limitations of claim 21. The Veriprint 2000 records department transfers (see above) in a *Verify Queue* (Veriprint User Guide, page 40), which serves as an *audit trail* (Veriprint User Guide, page 93). Thus, the Verify Queue can be seen as representing an “audit log data store”. In this way, the Veriprint 2000 sends company data information into an audit log data store. Taking cues from preceding discussion regarding claim 21, this audit log data store may just as well be stored on a central data center. Therefore, the time and attendance system, obtained by combining the teachings of

DiMaria et al. and the Veriprint User Guide, as discussed above, with the provision that the audit log data store (i.e. the Verify Queue) be stored on a central data center, would be in accordance with claim 22.

73. Claims 20 and 24-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over DiMaria et al., in view of Bonner et al. (U.S. Patent 5,842,182).

74. *The following is in regard to Claim 20.* As shown above, DiMaria et al. disclose a biometric time and attendance system that conforms to the biometric network of claim 18. DiMaria et al., however, do not expressly show or suggest sending employee information into an audit log data store in the central data center.

75. Bonner et al. disclose an automated system for tracking user time and attendance. In the system of Bonner et al., manual changes to a user's "time card" (i.e. transactional history) are logged in a "time card archive", thereby producing an "audit trail" of such manual changes. See, for example, Bonner et al. column 4, lines 35-42. In this manner, such a time card archive (i.e. time card archive 121 of Bonner et al. Fig. 3A) can be regarded as an "audit log data store". The time card archive is stored in memory 16 (Bonner et al. Fig. 1 and column 3, lines 25-28) connected to central processor 14. It should be understood that, since they are the primary sites of data processing and storage, the central processor (e.g. central processor 14 of Bonner et al. Fig. 1) and memory (e.g. memory 16 of Bonner et al. Fig. 1) constitute what can be reasonably considered a central data center. The audit log thus resides on a central data center, according to Bonner et al.

76. Bonner et al. and DiMaria et al. are combinable because they are analogous art. In particular, the teachings of Bonner et al. and DiMaria et al. are both directed toward time and attendance systems. Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the applicant's claimed invention, to supplement the biometric time and attendance system (or network) of DiMaria et al. with an audit log stored on a central data center (e.g. the host shown in DiMaria et al. Fig. 1), as suggested by Bonner et al. This would advantageously provide tracking of manual changes to a users transaction history. Clearly, this would, in turn, ensure data consistency and allow fraudulent changes to be accounted for. Incorporating an audit log stored on the central data center, as suggested by Bonner et al., into the time

and attendance system of DiMaria et al. would yield a biometric time and attendance system or network (see above) that adequately satisfies the limitations of claim 20.

77. *The following is in regard to Claim 24.* As shown above, DiMaria et al. disclose a biometric time and attendance system that conforms to the biometric network of claim 13. DiMaria et al., however, do not expressly show or suggest that manual changes can be made to entries in a transaction history.

78. Bonner et al. an automated system for tracking user time and attendance. As mentioned earlier, manual changes (e.g. “time card edits” – see, for example, Bonner et al. Fig. 3A reference number 118) are made to the transaction history of a user (i.e. a user’s “time card”) when these data deviate from what is expected (Bonner et al. column 4, lines 35-42).

79. Bonner et al. and DiMaria et al. are combinable because they are analogous art. In particular, the teachings of Bonner et al. and DiMaria et al. are both directed toward time and attendance systems. Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the applicant’s claimed invention, to program the system of DiMaria et al. to permit manual changes to entries in a transaction history, as suggested by Bonner et al. The software components that facilitate such operations could be considered collectively as a “manual transaction module”. One would have been motivated to perform such a modification of DiMaria et al.’s system because, by correcting “exceptions” (e.g. Bonner et al. Fig. 3A reference number 40), data consistency and/or correctness may be ensured. By programming the system of DiMaria et al. to permit manual changes to entries in a transaction history, as suggested by Bonner et al., one obtains a time and attendance network that conforms to that which is put forth in claim 24.

80. *The following is in regard to Claim 25.* As shown above, DiMaria et al. disclose a biometric time and attendance system that conforms to the biometric network of claim 24. It should be clear from the preceding discussions relating to claims 20 and 24 that time and attendance tracking according to Bonner et al. includes storing data related (i.e. the time card edits themselves – see Bonner et al. column 4, lines 35-42) to the manual entries (e.g. time card edits – see, for example, Bonner et al. Fig. 3A reference number 118) in an audit log data store (e.g. time card archive 121 of Bonner et al. Fig. 3A) in the central data center. Therefore, the biometric time and attendance network, obtained by combining the teachings of

DiMaria et al. and Bonner et al. in the manner discussed above, conforms to the proposed biometric time and attendance network of claim 25.

81. *The following is in regard to Claim 26.* As shown above, DiMaria et al. disclose a biometric time and attendance system that conforms to the biometric network of claim 24. As noted earlier, in the system of Bonner et al., manual changes to entries (i.e. time card edits) are added to the transaction history of a user (i.e. the user's time card – see Bonner et al. column 4, lines 35-42), which is stored at the central data center. Therefore, the biometric time and attendance network, obtained by combining the teachings of DiMaria et al. and Bonner et al. in the manner discussed above, conforms to the proposed biometric time and attendance network of claim 26.

82. Claims 27-28 and 33-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over DiMaria et al., in view of Wong et al. (U.S. Patent 6,119,933).

83. *The following is in regard to Claim 27.* As shown above, DiMaria et al. disclose a biometric time and attendance system that conforms to the biometric network of claim 13. DiMaria et al.'s system is further programmed to generate reports based on the time and attendance data. See, for example, step S9B shown in DiMaria et al. Fig. 3B. and column 4, lines 14-19. The components of DiMaria et al.'s system that are involved in report generation can be considered collectively as a "report generation module". However, report generation occurs at the host (i.e. the central data center), as opposed to at the client biometric device, in the system of DiMaria et al. That is, the report generation module is not part of the aforementioned software programmed *into the biometric device*.

84. Providing client-side report generation– i.e. at the biometric device or terminal – as opposed to at the central data center location, represents a relatively trivial distinction over DiMaria et al.'s system. Client-side report generation has been widely implemented in a multitude of client-server based data networks. For example, Wong et al. discuss biometric user verification in a client-server based POS (point-of-sale) system, wherein clients having biometric device (see Wong et al. Fig. 1) are capable of generating reports. See, for example, Wong et al. column 3, lines 57-59 and column 3, lines 65-67 to column 4, lines



1-10. These reports include time and attendance reports. See, for example, Wong et al. column 9, lines 53-54).

85. Wong et al. and DiMaria et al. are combinable because they are analogous art. In particular, the teachings of Wong et al. and DiMaria et al. are both directed toward client-server based data networks where users are verified by biometric input. Furthermore, the systems of Wong et al. and DiMaria et al. are employed in time and attendance applications. Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the applicant's claimed invention, to configure the biometric time and attendance system of DiMaria et al. to accommodate client-side (i.e. at the terminal) report-generation. The motivation to do so would have been to allow reports to be viewed or otherwise accessed at multiple and, perhaps more convenient, locations, as opposed to one central location. Configuring the time and attendance system of DiMaria et al., in this manner, would yield a system that generates time and attendance reports at the location of the biometric device. A system thus obtained would conform to claim 27.

86. *The following is in regard to Claim 28.* As shown above, the system, obtained by combining the teachings of DiMaria et al. and Wong et al. in the manner discussed above, adequately satisfies the limitations of claim 27. Furthermore, the reports generated by DiMaria et al.'s system include date and time of entry/exit (i.e. information from the aforementioned transaction history data store) and an individual's identity (i.e. information from the aforementioned employee information data store). See DiMaria et al. column 4, lines 14-19. Therefore, the system, obtained by combining the teachings of DiMaria et al. and Wong et al. in the manner discussed above, conforms to that which is put forth in claim 28.

87. *The following is in regard to Claim 33.* As shown above, DiMaria et al. disclose a biometric time and attendance system that conforms to the biometric system of claim 29. Also shown above (e.g. the discussion relating to claim 27), the system of DiMaria et al. a report including at least a portion of the time and attendance data. Since, in the system of DiMaria et al., the report is generated by the host, the generated report contains time and attendance data generated by the host, not necessarily by the biometric device (terminal).

88. Providing client-side report generation— i.e. at the biometric device or terminal – as opposed to at the central data center location, represents a relatively trivial distinction over DiMaria et al.'s system. Client-side report generation has widespread implementation in a multitude of client-server based data networks. For example, Wong et al. discuss biometric user verification in a client-server based POS (point-of-sale) system, wherein clients having biometric device (see Wong et al. Fig. 1) are capable of generating reports. See, for example, Wong et al. column 3, lines 57-59 and column 3, lines 65-67 to column 4, lines 1-10. These reports include time and attendance reports. See, for example, Wong et al. column 9, lines 53-54). Also note that the reports contain client-generated data. See, for example, Wong et al. column 4, lines 5-6.

89. Wong et al. and DiMaria et al. are combinable because they are analogous art. In particular, the teachings of Wong et al. and DiMaria et al. are both directed toward client-server based data networks where users are verified by biometric input. Furthermore, the systems of Wong et al. and DiMaria et al. are employed in time and attendance applications. Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the applicant's claimed invention, to configure the biometric time and attendance system of DiMaria et al. to accommodate client-side (i.e. at the terminal) report-generation. The motivation to do so would have been to allow reports to be viewed or otherwise accessed at multiple and, perhaps more convenient, locations, as opposed to one central location. Configuring the time and attendance system of DiMaria et al., in this manner, would yield a system that generates time and attendance reports at the location of the biometric device. These reports would, therefore, include at least a portion of the time and attendance data generated by the biometric device. A system thus obtained would conform to claim 33.

90. *The following is in regard to Claim 34.* As shown above, DiMaria et al. disclose a biometric time and attendance system that conforms to the biometric system of claim 31. Claim 34 distinguishes itself from claim 33 by specifying that the source of biometric data is a user's fingerprint. Therefore, arguments presented above with regard to claims 33 are applicable here. Given those arguments and the fact that a fingerprint is the biometric source of choice in DiMaria et al.'s system (DiMaria et al. column 3, lines 57-58), the biometric time and attendance system of DiMaria et al. conforms to biometric system proposed in claim 34.

91. Claims 6, 10, and 35-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over DiMaria et al., in view of Gullman et al. (U.S. Patent 5,280,527).

92. *The following is in regard to Claim 35.* DiMaria et al. discloses a biometric time and attendance system that includes:

(35.a.) At least one biometric unit capable of comparing user live biometric data with stored biometric data and generating data related to the user. See the discussion above relating to (1.a), (1.c), and claim 4.

(35.b.) A central data center in communication with the biometric device to receive and process the data. See the discussions above relating to (1.b) and (55.d)-(55.e).

DiMaria et al. et al., however, do not show or suggest the usage of a plurality of biometric tokens<sup>1</sup> having biometric data, stored thereon, specific to a user. DiMaria et al. also fail to show or suggest the comparison of the live biometric data to the biometric data stored on the biometric tokens.

93. Gullman et al., on the other hand, disclose a biometric token for authorizing access to a host system. This biometric token is presented to an access device (e.g. access device 12 in Gullman et al. Fig. 1 – note the similarity to the terminal 100 of DiMaria et al.). The biometric token is in the form of an integrated circuit card and has a biometric template, attributed to the cardholder, stored thereon. See, for example, Gullman et al. column 2, lines 49-53. In order to verify the user, comparison is then made between the biometric template stored on the token and the live biometric data. See, Gullman et al. column 3, lines 49-55. In this case, one can consider the access device 12 and security mechanism 14 (i.e. the token) of Gullman et al. Fig. 1 as collectively constituting a biometric device.

---

<sup>1</sup> Note that the word *token* has several meanings particular to the realms of networking, database and security system technologies. Token will be assumed to mean a small device (e.g. a smart card) the size of a credit card that contains a constantly changing ID code (also frequently referred to as a token). This interpretation of the word token is consistent with the language of the claims, as well as its usage in the latter of the aforementioned technologies. To avoid confusion, the changing ID code will be referred to as a *token code*.

94. The teachings of Gullman et al. and DiMaria et al. are combinable because they are analogous art. Specifically, both the teachings of Gullman et al. and DiMaria et al. are both directed to systems consisting of a host and at least one terminal having biometric sensors for user verification. Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the applicant's claimed invention, to use biometric tokens, such as those of Gullman et al., in the system of DiMaria et al., and compare live biometric data against the individualized biometric data stored on these tokens for the purposes of user verification. The motivation to do so would have been to provide reliable and secure identification that eliminates the need for a user to memorize codes (Gullman et al. column 6, lines 48-50). It should be apparent that the token-codes (e.g. biometric correlation factor concatenated with a fixed or time-varying code – Gullman et al. column 4, lines 3-11) of Gullman et al., provide additional security over comparing stored and live biometric data alone. By utilizing biometric tokens, in the time and attendance system of DiMaria et al., according to the preceding discussion, one obtains a network<sup>2</sup> that conforms that of claim 35.

95. *The following is in regard to Claim 36.* As shown above, the teachings of Gullman et al. and DiMaria et al., when combined in the manner discussed above, satisfy the limitations of claim 35. As discussed above (see the discussion above regarding claim 46), data generated by the system of DiMaria et al. includes user entry time, user exit time, user check-in time and user attendance information. Therefore, by utilizing biometric tokens, in the time and attendance system of DiMaria et al., according to the preceding discussion, one obtains a network that is in accordance with claim 36.

96. *The following is in regard to Claim 6.* As shown above, DiMaria et al. disclose a biometric time and attendance system that conforms to the biometric system of claim 1. DiMaria et al. et al., however, do not show or suggest that the stored biometric data be stored on one of an optical card, data card, memory card, smart card, biometric token, or storage button.

---

<sup>2</sup> See the discussion above relating to the *network* of claim 13.

97. Gullman et al., on the other hand, disclose a biometric token for authorizing access to a host system. This biometric is presented to an access device (e.g. access device 12 in Gullman et al. Fig. 1 – note the similarity to the terminal 100 of DiMaria et al.). The biometric token is in the form of an integrated circuit card and has a biometric template, attributed to the cardholder, stored thereon. See, for example, Gullman et al. column 2, lines 49-53.

98. The teachings of Gullman et al. and DiMaria et al. are combinable because they are analogous art. Specifically, both the teachings of Gullman et al. and DiMaria et al. are both directed to systems consisting of a host and at least one terminal having biometric sensors for user verification. Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the applicant's claimed invention, to use biometric tokens, such as those of Gullman et al., in the system of DiMaria et al. in order to store the stored biometric data. Using biometric tokens in this way, within the system of DiMaria et al., would yield a time and attendance system that conforms to that which is proposed in claim 6.

99. *The following is in regard to Claim 10.* As shown above, DiMaria et al. disclose a biometric time and attendance system that conforms to the biometric system of claim 1. Note that a wireless data card can be considered one of an optical card, data card, memory card, smart card, biometric token, or storage button. As discussed above with regard to claim 6, Gullman et al. disclose a wireless data card (see Gullman et al. Fig. 3) having biometric templates stored thereon. Therefore, with regard to claim 10, arguments presented above relative to claim 6 are applicable.

100. Claims 37-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over DiMaria et al., in view of Gullman et al., in further view of Schenker et al. (U.S. Patent 6,633,223).

101. *The following is in regard to Claims 37-39.* As shown above, the teachings of Gullman et al. and DiMaria et al., when combined in the manner discussed above, satisfy the limitations of claim 35. Neither Gullman et al. nor DiMaria et al. show or suggest that the user be either a student, teacher, or authorized student guardian. More generally, neither Gullman et al. nor DiMaria et al. show or suggest the application of time and attendance systems, such as those discussed extensively above, to classroom settings.

102. Schenker et al. discloses a system for monitoring student movement (i.e. movement between classes) and attendance (Schenker et al. Abstract) that consists of a central data center (e.g. LAN database or mainframe 11 of Schenker et al. Fig. 2). Schenker et al.'s system is essentially a student time and attendance system. Furthermore, Schenker et al.'s system uses a token having biometric information stored thereon (e.g. "substrate having encoded indicia correlateable with the image of the student", where the image represents biometric information – see Schenker et al. column 6, lines 15-20). The token and the information stored thereon (including the biometric information) is used to verify a student's identity (see Schenker et al. column 6, lines 24-26). Therefore, Schenker et al. shows a time and attendance system, similar in structure and operation to that of DiMaria et al., being used within a classroom/school environment.

103. The teachings of Schenker et al. are combinable with those of Gullman et al. and DiMaria et al. because they are analogous art. More particularly, the systems of Schenker et al. and DiMaria et al. are essentially time and attendance systems of similar structure and operation employing biometrics in at least part of the user verification process. The teachings of Schenker et al. and Gullman et al. both concern biometric tokens, having biometric information stored thereon, that are used for user verification within a client/server data network environment. Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the applicant's claimed invention, to deploy the time and attendance system (network), obtained by combining the teachings of DiMaria et al. and Gullman et al. as extensively discussed above, within a classroom/school environment. The motivation to do so would have been to provide a robust, reliable, and automated means to monitor the attendance of students, school personnel, and other educational participants.

104. Clearly, Schenker et al. suggests that students be users of such time and attendance networks or systems. Furthermore, it would have been obvious to one of ordinary skill in the art, at the time of the applicant's claimed invention, that teachers, having a need to monitor their students' attendance, should also be included as users. Similarly, authorized student guardians should also be allowed to access such systems. Allowing students, teachers, and/or authorized student guardians to access the time and attendance system (network), obtained by combining the teachings of DiMaria et al. and Gullman et al., and deployed in a classroom or school, as suggested by Schenker et al., would have been well within the capabilities

of one of ordinary skill in the art. A system or network thus obtained would be in accordance with that which is put forth in claims 37-39.

105. Claims 40-41 and 53 are rejected under 35 U.S.C. 103(a) as being unpatentable over DiMaria et al., in view of Schenker et al.

106. *The following is in regard to Claim 40.* DiMaria et al. disclose a time and attendance system that includes:

- (40a.) At least one biometric unit that compares live biometric data with stored biometric data to generate time and attendance data.
- (40.b.) A central data center in communication with the biometric device.
- (40.c.) The generated data relates to time and attendance information with respect to the user.

See the discussion above with regard to claim 1. Also see the discussion above relating the network of claim 13 and note that the system of DiMaria et al. can be considered a network. DiMaria et al., however, does not teach the usage of such a time and attendance network within a classroom or school setting.

107. Schenker et al. discloses a system for monitoring student movement (i.e. movement between classes) and attendance (Schenker et al. Abstract) that consists of a central data center (e.g. LAN database or mainframe 11 of Schenker et al. Fig. 2). Schenker et al.'s system is essentially a student time and attendance system. Furthermore, Schenker et al.'s system uses a token having biometric information stored thereon (e.g. "substrate having encoded indicia correlateable with the image of the student", where the image represents biometric information – see Schenker et al. column 6, lines 15-20). The token and the information stored thereon (including the biometric information) is used to verify a student's identity (see Schenker et al. column 6, lines 24-26). Therefore, Schenker et al. shows a time and attendance system, similar in structure and operation to that of DiMaria et al., being used within a classroom/school environment. Clearly, by tracking *class* attendance, Schenker et al. impliedly suggests that, in such a classroom/school time and attendance network, the biometric devices (e.g. optical reader 34 of Schenker et al. Fig. 2) be present in a classroom.

108. The teachings of Schenker et al. are combinable with those of DiMaria et al. because they are analogous art. More particularly, the systems of Schenker et al. and DiMaria et al. are essentially time and attendance systems of similar structure and operation employing biometrics in at least part of the user verification process. Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the applicant's claimed invention, to deploy the time and attendance system (network) of DiMaria et al., within a classroom/school environment. The motivation to do so would have been to provide a robust, reliable, and automated means to monitor the attendance of students, school personnel, and other educational participants. Adapting the time and attendance system (network) of DiMaria et al. to an academic setting would yield a classroom time and attendance network, including elements (40.a)-(40.c), where the biometric devices are located in the classroom. Such a classroom time and attendance network would be in accordance with claim 40.

109. *The following is in regard to Claim 41.* As shown above, the teachings of Schenker et al. and DiMaria et al., when combined in the manner discussed above, satisfy the limitations of claim 40. As shown above with respect to claims 30, 32, and 36, the data generated in DiMaria et al.'s system includes user entry time, user exit time, user check-in time and user attendance. Therefore, the classroom time and attendance network, obtained by combining the teachings of Schenker et al. and DiMaria et al. in the manner discussed above, would conform to that which is put forth in claim 40.

110. *The following is in regard to Claim 53.* As shown above, DiMaria et al. disclose a biometric time and attendance method that conforms to the method of claim 52. DiMaria et al., however, does not teach that the user is one selected from the group consisting of a student, teacher, professor, authorized child custodian, parent, therapist or school-related personnel.

111. Schenker et al. discloses a methodology for monitoring student movement (i.e. movement between classes) and attendance (Schenker et al. Abstract) that consists of a central data center (e.g. LAN database or mainframe 11 of Schenker et al. Fig. 2). Schenker et al.'s methodology is essentially a student time and attendance method, utilizing biometric user verification (the user image represents biometric information used for verification – see Schenker et al. column 6, lines 15-20). Therefore, Schenker et al. demonstrates the usage of a time and attendance method, utilizing biometric user verification, within an academic setting.



Clearly, students represent one class of users that may access the time and attendance system or method of Schenker et al.

112. The teachings of Schenker et al. are combinable with those of DiMaria et al. because they are analogous art. More particularly, the methods of Schenker et al. and DiMaria et al. are essentially time and attendance methods of similar functionality employing biometrics in at least part of the user verification process. Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the applicant's claimed invention, to deploy the time and attendance system (network) or methodology of DiMaria et al., within a classroom/school environment. Given demonstrated applicability of time and attendance systems/methods to academic environments, it would have also been obvious to one of ordinary skill in the art, at the time of the applicant's claimed invention, to include other academic participants and personnel, such as teachers, professors, authorized child custodians, parents, therapists or school-related personnel, as users with access to the time and attendance system. The motivation to do so would have been to provide a robust, reliable, and automated method to monitor the attendance of students, school personnel, and other educational participants. Adapting the time and attendance method of DiMaria et al. to be operable within an academic context and further making it accessible to the various academic participants mentioned above, would yield a method that conforms to claim 53.

113. Claim 59 is rejected under 35 U.S.C. 103(a) as being unpatentable over DiMaria et al., in view of Bennett (U.S. Patent 5,550,359).

114. *The following is in regard to Claim 59.* As shown above, DiMaria et al. disclose a biometric time and attendance method that conforms to the method of claim 55. DiMaria et al., however, does not expressly show or suggest that the data from the biometric devices be received periodically.

115. Bennett discloses a time and attendance system consisting of a reader(s) (reader 10 of Bennett Fig. 1) connected to a host(s), where time and attendance data is archived. See Bennett column 3, lines 55-63. Note that the reader(s) and host(s) of Bennett's system are respectively analogous to the biometric terminal(s) (e.g. terminals 20, DiMaria et al. Fig. 1) and host (e.g. host 20, DiMaria et al. Fig. 1) of DiMaria et al.'s system. In Bennett's time and attendance system, the reader(s) are polled periodically by a host,

thereby retrieving time and attendance data stored on the reader. See Bennett Fig. 8 and column 9, lines 62-67 to column 10, lines 1-4.

116. Bennett and DiMaria et al. are combinable because they are analogous art. In particular, the teachings of Bennett and DiMaria et al. are both directed toward time and attendance systems and methods. Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the applicant's claimed invention, to modify the time and attendance system/method of DiMaria et al., according to the teachings of Bennett, so that the host (i.e. the central data center) polls (i.e. retrieves time and attendance data) from the biometric devices (e.g. terminals 10 of DiMaria et al. Fig. 1) periodically. The advantage of polling schemes such as these is that they are functionally simple. Furthermore, since data is transmitted periodically at predetermined intervals, network traffic is deterministic and network bandwidth is conserved. Such a modification to the time and attendance methodology of DiMaria et al. would result in a method in accordance with claim 59.

117. Claim 60 is rejected under 35 U.S.C. 103(a) as being unpatentable over DiMaria et al., in view of Swart (U.S. Patent 6,330,594).

118. *The following is in regard to Claim 60.* As shown above, DiMaria et al. disclose a biometric time and attendance method that conforms to the method of claim 55. Although it is reasonable to assume that the data (e.g. biometric data, user identification and/or time and attendance data), generated at the terminal of DiMaria et al.'s system, is received in real-time (that is, immediately after it is available at the terminal), DiMaria et al. does not expressly show or suggest that the data from the biometric devices be received in real-time.

119. According to Swart (Swart column 4, lines 59-67 to column 5, lines 1-6), "data acquisition systems [e.g. biometric time and attendance systems such as that of DiMaria et al.]... are used by many business in the private and public sector for monitoring applications such as monitoring working time and attendance of employees ... These systems include real-time data input devices [e.g. biometric terminals 10 depicted in DiMaria et al. Fig. 1] or data collection readers such as card swipes, data entry readers, turnstiles, garage parking gates, etc. connected to real-time server units. The server units interface ... can

monitor, for example, employee activities at a work site by tracking a plurality of real-time events such as entry and exits through given access doors, turnstiles, vehicle barriers, etc.”. This suggests real-time communication of data between data input devices (e.g. biometric terminals 10 depicted in DiMaria et al. Fig. 1) and server units (e.g. host 20 depicted in DiMaria et al. Fig. 1), in applications such as time and attendance systems.

120. The teachings of Swart are combinable with those of DiMaria et al. because they are analogous art. While the teachings of Swart generally relate to network computing, and more particularly to a method and apparatus for interfacing with, controlling and accessing real-time data acquisition systems, the excerpt above, clearly show their amenability to time and attendance applications, such as DiMaria et al.’s time and attendance system and methodology. Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the applicant's claimed invention, to use real-time communication (i.e. via real-time input devices, such as the aforementioned biometric terminals, in conjunction with real-time server units) of data between the terminals and host of DiMaria et al.’s biometric time and attendance system and method. This is in accordance with Swart’s suggestion above. The motivation to do so would have been to ensure the host or server-side time and attendance data responsive to real-time events, thereby providing a real-time view of the time and attendance of the system’s users. Configuring the biometric time and attendance method and system of DiMaria et al. for real-time communication between the host and terminals would result in a system that adequately satisfies the limitations of claim 60.

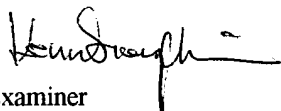
---

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Siangchin whose telephone number is (703)305-7569. The examiner can normally be reached on 9:00am - 5:30pm, Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Amelia Au can be reached on (703)308-6604. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Kevin Siangchin



Examiner  
Art Unit 2623

ks - 06/23/04



AMELIA M. AU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2623